

CLAIMS

What is claimed is:

1. A method for use in a computer capable of supporting multiple authentication mechanisms, the method comprising:

generating at least one indicator associated with and identifying at least one authentication mechanism; and

controlling access to at least one resource based on the indicator.

2. The method as recited in Claim 1, wherein generating the indicator further includes receiving inputs, providing the inputs to the authentication mechanism, and causing the authentication mechanism to generate at least one security identifier (SID) that identifies the authentication mechanism.

3. The method as recited in Claim 1, wherein generating the indicator further includes identifying within the indicator at least one characteristic associated with the authentication mechanism.

4. The method as recited in Claim 3, wherein the at least one characteristic associated with the authentication mechanism includes a measure of strength of the authentication mechanism.

5. The method as recited in Claim 4, wherein the measure of strength of the authentication mechanism identifies a length of an encryption key employed by the authentication mechanism.

1 6. The method as recited in Claim 1, wherein controlling access to the
2 resource based on the indicator further includes comparing the indicator to at least
3 one access control list having at least one access control entry therein.

4
5 7. The method as recited in Claim 6, wherein if the access control entry
6 operatively specifies that the at least one authentication mechanism is permitted to
7 access the resource, then access to the at least one resource is allowed to proceed.

8
9 8. The method as recited in Claim 6, wherein if the access control entry
10 operatively specifies that the at least one authentication mechanism is not
11 permitted to access the resource, then access to the at least one resource is not
12 allowed to proceed.

13
14 9. The method as recited in Claim 6, wherein if the access control entry
15 does not operatively specify that the at least one authentication mechanism is
16 permitted to access the resource, then access to the at least one resource is not
17 allowed to proceed.

18
19 10. The method as recited in Claim 1, wherein the indicator includes a
20 security token.

21
22 11. A computer-readable medium for use in a device capable of
23 supporting multiple authentication mechanisms, the computer-readable medium
24 having computer-executable instructions for performing acts comprising:
25

1 producing at least one indicator that uniquely identifies at least one
2 authentication mechanism supported by the device; and

3 causing the device to selectively control access to at least one resource
4 operatively coupled to the device based at least in part on the indicator.
5

6 12. The computer-readable medium as recited in Claim 11, wherein
7 producing the indicator further includes receiving inputs, providing the inputs to
8 the authentication mechanism, and causing the authentication mechanism to
9 generate at least one security identifier (SID) that identifies the authentication
10 mechanism, in response thereto.
11

12 13. The computer-readable medium as recited in Claim 11, wherein
13 producing the indicator further includes identifying within the indicator at least
14 one characteristic of the authentication mechanism.
15

16 14. The computer-readable medium as recited in Claim 13, wherein the
17 at least one characteristic of the authentication mechanism includes a strength
18 characteristic of the authentication mechanism.
19

20 15. The computer-readable medium as recited in Claim 14, wherein the
21 strength characteristic identifies a length of an encryption key employed by the
22 authentication mechanism.
23

24 16. The computer-readable medium as recited in Claim 11, wherein
25 causing the device to selectively control access to the at least one resource based

1 on the indicator further includes causing the device to compare the indicator to
2 control data .
3

4 17. The computer-readable medium as recited in Claim 16, wherein if
5 the control data specifies that the authentication mechanism is permitted to access
6 the resource, to which subsequent access to the resource is allowed.
7

8 18. The computer-readable medium as recited in Claim 16, wherein if
9 the control data operatively specifies that the authentication mechanism is not
10 permitted to access the resource, to which subsequent access to the resource is
11 prohibited.
12

13 19. The computer-readable medium as recited in Claim 16, wherein if
14 the control data does not operatively specify that the authentication mechanism is
15 permitted to access the resource, to which subsequent access to the resource is
16 prohibited.
17

18 20. The computer-readable medium as recited in Claim 10; wherein the
19 indicator includes a security token.
20

21 21. An apparatus comprising:

22 at least one authentication mechanism configured to generate at least one
23 indicator that identifies the authentication mechanism;

24 an access control list;

25 at least one access controlled resource; and

1 logic operatively configured to compare the indicator with the access
2 control list and selectively control access to the resource based on the indicator .
3

4 22. The apparatus as recited in Claim 21, wherein the authentication
5 mechanism is further configured to receive user inputs and generate at least one
6 security identifier (SID) that identifies the authentication mechanism based on the
7 user inputs.
8

9 23. The apparatus as recited in Claim 21, wherein the indicator further
10 includes at least one identifying characteristic associated with the authentication
11 mechanism.
12

13 24. The apparatus as recited in Claim 23, wherein the at least one
14 identifying characteristic associated with the authentication mechanism indicates a
15 measure of strength of the authentication mechanism
16

17 25. The apparatus as recited in Claim 24, wherein the measure of
18 strength of the authentication mechanism identifies a length of an encryption key
19 employed by the authentication mechanism.
20

21 26. The apparatus as recited in Claim 23, wherein the indicator includes
22 a security token.
23
24
25